F. Information Outputs

[0081] Referring again to FIG. **6** and FIG. **7**, upon performing above-described facial recognition process, the system may identify one or more matching candidate images with different degrees of match (for example, as measured by distance values) in an image database. The system may also retrieve the profile information stored in a personal data database. The profile information can be retrieved by the system from the personal data database include, without limitation, a name, a gender, a date of birth or an age, a place of birth a nationality, a correspondence language, a civic address, a phone number, an email address, an instant messaging identifier, financial information, marital status, hobbies, favorite sports teams, education, educational degrees, universities, and information posted by others. The profile information may also include a link to a webpage on a website containing the information related to a person of interest. For example, the website can be a social networking website, a professional networking website, a personal website, or an employer website. The system may include a privacy settings module that operates to establish a privacy setting for individuals to access a database.

[0082] In some embodiments, the personal information is retrieved from the database based on a predetermined privacy setting of the identified candidate. In some embodiments, the method further includes displaying one or more facial images of the identified candidate and the personal information associated therewith. In some embodiments, the method may also include transmitting a notification to the user device if the identified candidate poses a high risk to the public or is a criminal. In some embodiments, the personal information may include a name of the identified candidate. In some embodiments, the personal information may include a link to an online profile associated with the identified match. In some embodiments, the personal information transmitted to the user device is obtained from a webpage having the highest PageRank value among the webpages containing the personal information.

[0083] The information provided by the system may be used to determine the identity of individuals. For example, the information can be used to identify a person of interest. A person of interest may include a person announce missing, a person accused of a crime, a person with a criminal record, a sex offender, a person who has suffered memory loss, and a person who may otherwise poses a high risk to the public. In one example, the information can be used by social workers to identify homeless people or people in need. Likewise, law enforcement may use the facial recognition system to identify information about a person. By accurately identifying a person, and dynamically an in real-time obtaining information about the person, more accurate decisions may be made. Social benefits may be accurately dispensed, thereby reducing fraud. Law enforcement may use information about a person to learn if they have a medical condition or mental issue or handicap that may prevent them from responding or cause them to act inappropriately. Police may react differently to a person with no arrest record and a medical condition, and a person facially detected to have a history of assaulting police. A person with a history of DUI arrests, revealed by the facial scans, may be treated differently than a person with a history of diabetic low blood sugar symptoms. A simple facial scan can provide the identity of a person even if that person eludes capture by the police.

G. Other Applications

(i) Identification Verification Based on Facial Recognition

[0084] In another aspect, this disclosure also provides a method for verifying personal identification based on facial recognition. The disclosed system enables individuals to be instantly identified and approved/disapproved for entry into a venue (e.g., a building, a bank, a facility, a lab, a secured location). The system is entirely face-based and can be seamlessly implemented. It does not require downloading an app or interaction with a touch screen. The individual simply looks at the camera or a mobile device (e.g., mobile phone, iPad) and is then approved or disapproved. The system also keeps an automated log of individuals entering/leaving the building according to face, name, and date/time.

[0085] The method can be used to grant or deny access for a person to a facility, a venue, or a device. As described above, the system may include components that capture an image of a person, and then with associated circuitry and software, process the image and then compare the image with stored images, if desired. In a secured access environment, a positive match between the acquired image of the individual and a pre-stored image allows access to the facility.

[0086] In some embodiments, the method also includes (i) determining permission of access for the subject to a venue or an account based on the personal information of the identified candidate; (ii) granting the access for the subject if the identified candidate is an authorized user, or denying the access for the subject if the identified candidate is not an authorized user or a candidate matching the captured facial image cannot be identified; and (iii) transmitting a message indicative of granting or denying the access to the venue or the account. In some embodiments, the account is associated with a bank, a financial institute or a credit company.

[0087] In another aspect, this disclosure provides a method for verifying an identity of a user. For example, individual users can create their own personal "face file" that includes their headshot and a secure personal identification number (PIN). The individual can use the file/account as a form of highly secure, theft-proof facial/biometric identification for their day-to-day transactions.

[0088] In some embodiments, the method includes (a) providing a facial image data comprising a captured facial image and a personal identification number of the user; (b) transforming the facial image data to facial recognition data; (c) comparing the facial recognition data and the personal identification number to reference facial recognition data and reference personal identification numbers associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image and the personal identification number; and (d) upon identification of the candidate, transmitting a confirmation to a user device indicating the user is an authorized user.

(ii) Facial Data Collaborative Network and Correlative Face Search

[0089] In yet another aspect, the method additionally includes providing access to the database to a plurality of users. The plurality users may be located in the same geographic area or associated with the same business type. The system enables the networking of groups of clients